# LevelBlue - Open Threat Exchange

By msudosos

Archived: 2026-04-02 10:45:03 UTC

- 39 Subscribers

- 133 Subscribers

- 133 Subscribers

## ACTIVIDAD MALICIOSA | Relacionada con Amadey 05-05-2025

**FileHash-MD5:** 60 | **FileHash-SHA1:** 61 | **FileHash-SHA256:** 60 | **URL:** 5 | **YARA:** 1

If you want to create an interactive image, try Genially, a free online design and design app that lets you design, create and create interactive images for your friends, family and friends..

- 26 Subscribers

- 224 Subscribers

## Black Tech

**CIDR:** 1 | **CVE:** 37 | **FileHash-MD5:** 2449 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 3441 | **URL:** 2044 | **Domain:** 258 | **Email:** 4 | **Hostname:** 1100

Found in a malicious Apple iTunes link. Lists several independent artists. Music "producer" is potentially highly dependent on use of AI generated instrumentation and conception. Hacking seems to target a single target and associates.

- 224 Subscribers

## Qbot

**CVE:** 10 | **FileHash-MD5:** 1424 | **FileHash-SHA1:** 983 | **FileHash-SHA256:** 3174 | **URL:** 3167 | **Domain:** 4091 | **Email:** 25 | **Hostname:** 2422

- 224 Subscribers

## BazaarLoader | REDCAP | https://jbplegal com/ | Cyber espionage

**CVE:** 5 | **FileHash-MD5:** 2428 | **FileHash-SHA1:** 2136 | **FileHash-SHA256:** 5377 | **SSLCertFingerprint:** 4 | **URL:** 2401 | **Domain:** 3794 | **Email:** 19 | **Hostname:** 2763

Found periphery.m (moderate sized dump) Targets Tsara Brashears Several staffed law offices based on Colorado, USA. Contact made. Physical records. Client: Brashears. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Trojan.Win32.REDCAP.MCRK/ 1c597b7c7934ef03eb0def0b64655dd79abe08567ff3053761e5516064a43376 https://otx.alienvault.com/malware/TEL:Trojan:Win32%2FBazaarLoader!MTB/ https://www.trendmicro.com/en_ph/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html TEL:Trojan:Win32/BazaarLoader 987204ca82337f0a3f28097a5d66d5f3ecb11d43d82f67cd753d0bf2ce40b7a7

- 224 Subscribers

- 224 Subscribers

- 480 Subscribers

- 218 Subscribers

## [Nokoyawa Ransomware - https://house.mo.gov/]

**CVE:** 4 | **FileHash-MD5:** 194 | **FileHash-SHA1:** 191 | **FileHash-SHA256:** 2376 | **URL:** 4388 | **Domain:** 1414 | **Email:** 5 | **Hostname:** 1699

Cyber attack including Pegasus found in https://house.mo.gov/ This Observed links: dns.msftncsi.com • https://dns.msftncsi.com/ • http://dns.msftncsi.com/Appears to attacking with heightened privilege escalation. Links originated from https://safebae.org attack, various Westlaw links and links attacking a private citizen. HallRender is malware hosting domain featuring an aggressive 'Brian Sabey' representing self as attorney protecting white collar individuals accused of SA is attacker. Boldly contacts victims via mail, email, phone, text, invites, personal invitations to office. Front facing https://safebae.org, a 'tribute' domain may mention alleged SA victim Daisy Coleman. Research confirms no mention of 'Daisy' safebae is filled with cyber bullying toolkit; ransomware.csv, tracking, westlaw, tagging tools, pornhub, rallypoint, adult malvertizing content targeting a Colorado SA victim. It's all very real but so unbelievable. Malware spreading, cyberthreat

- 218 Subscribers

- 224 Subscribers

## VirTool:Win32/AccessMe | Ghost RAT

**CVE:** 1 | **FileHash-MD5:** 143 | **FileHash-SHA1:** 130 | **FileHash-SHA256:** 1524 | **SSLCertFingerprint:** 2 | **URL:** 3340 | **Domain:** 1735 | **Email:** 6 | **Hostname:** 1398

- 224 Subscribers

- 224 Subscribers

## Honeypot | https://jbplegal com/ | Cyber espionage | DynamicLoader,

**CVE:** 5 | **FileHash-MD5:** 2213 | **FileHash-SHA1:** 1921 | **FileHash-SHA256:** 4239 | **SSLCertFingerprint:** 4 | **URL:** 1509 | **Domain:** 3480 | **Email:** 17 | **Hostname:** 2466

Found periphery.m (moderate sized dump) Targets Tsara Brashears Several staffed law offices based on Colorado, USA. Contact made. Physical records. Client: Brashears. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Trojan.Win32.REDCAP.MCRK/ 1c597b7c7934ef03eb0def0b64655dd79abe08567ff3053761e5516064a43376 https://otx.alienvault.com/malware/TEL:Trojan:Win32%2FBazaarLoader!MTB/ https://www.trendmicro.com/en_ph/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html TEL:Trojan:Win32/BazaarLoader 987204ca82337f0a3f28097a5d66d5f3ecb11d43d82f67cd753d0bf2ce40b7a7https://www.joesandbox.com/analysis/1311477 Target: Critical Risk. In person contact made. Fraud services offered. This is crazy.

- 224 Subscribers

- 218 Subscribers

- 218 Subscribers

- 218 Subscribers

## PEXE - DOS executable (COM)

**CVE:** 2 | **FileHash-MD5:** 153 | **FileHash-SHA1:** 71 | **FileHash-SHA256:** 1690 | **URL:** 9526 | **Domain:** 4882 | **Email:** 250 | **Hostname:** 6120

- 218 Subscribers

---

Source: https://otx.alienvault.com/browse/pulses?q=tag:DNSpionage